الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مركز الدراسات الاستراتيجية للأمن السيبراني
Center For Cybersecurity Strategic Studies

Cybersecurity Quarterly Bulletin

Q4 2019

Classification: Open
TLP: White

Contents

Highlights from the Quarter

This section offers a brief overview of key takeaways from Q4 2019 (October-December)

Ransomware remains a global threat – Although the number of ransomware attacks declined in 2019 (at least 5%), the average ransom grew, reaching 3,500,000+SAR , in certain cases.This is due to the fact that key sectors are globally targeted, such as healthcare, aiming for higher returns per single attack.

Cost of data breaches continues to grow – This holds true for smaller organizations (>1.000 employees), lacking access to the most qualified professionals, and has particular impact on organizations in the MENA region, registering a 50% higher figure than a particular global average.

Disinformation grows – The trend is enabled by new technologies and social media. The phenomenon is unlikely to decrease in the near future.

Quantum computing's challenges – In a decade, quantum computing will provide unimaginable computing power. In particular, it will challenge cryptography, and the speed of machines to be able to break algorithms

Bits and Bytes

Key quarterly statistics, top threats and targeted sectors globally

Cybersecurity workforce needs to grow

145%

51%+ of cybersecurity professionals believe staff shortages expose organizations to security risks.[1]

Cyber Attacks growth

+60% last year

In 2019, 170+ of government entities were hit globally. Experts expect this to increase in 2020.

Average cost of data breaches to SMEs** is

13,255 SAR/employee

for organizations with 500-1000 employees. Bigger entities (25,000+ employees) face lower costs, approx. 765 SAR/employee.[3]

Average cost of breached records in MENA is

38,000+ SAR/per breach

50% higher than the global average of 25,757 records.[4]

Top 5 targeted sectors globally in Q4 20195

1. Public : 17.9%
2. Healthcare: 17.6%
3. Finance: 10.4%
4. Education: 10.1%
5. Science & technology: 9.8%

Top 5 threats in KSA in Q4 20196

- Malware
- Unauthorized access
- Inappropriate use
- Penetration/attempt to penetrate
- Data Leakage

[1] ISC2, Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)2 Cybersecurity Workforce Study, 2019, p. 8.
[3] Cost of Data Breach Report 2019, Ponemon Institute and IBM Security, p. 7.
[4] Cost of Data Breach Report 2019, Ponemon Institute and IBM Security, p. 10.
[5] Numbers show the distribution (%) over the total number of attacks registered worldwide for Q4.
[6] NCA analysis. Numbers show the top cybersecurity threats registered in the Kingdom of Saudi Arabia for Q4.

* Middle East and North Africa
** Small-Medium Enterprises

Global Cyber Outlook

Cybersecurity headlines from around the world

Ransomware named top threat in 2019 according to Europol

Europol recently published the 2019 "Internet Organised Crime Threat Assessment" report. According to the report, ransomware remains a top threat globally. However, methods are changing, focusing on targeted victims with techniques such as spear phishing, in an attempt to pursue higher gains with less effort.[7] As a result, the total number of attacks decreased in 2019, but the value of average ransom grew. This is confirmed by data from the private sector, highlighting a year-on-year drop of 5%, down to 150 million attacks.[8]

Europol also published a report entitled "Spear Phishing. A Law Enforcement and Cross-Industry Perspective," in which it emphasized the dangers of spear phishing to organizations of all sizes.[9] The report highlights the importance of adequate technical defences, training and awareness, and stresses the need for cooperation, particularly with law enforcement.

Atlantic Council publishes the results of the first global survey on aviation cybersecurity

The report, entitled "Aviation Cybersecurity: Scoping the Challenge," highlights a number of challenges for the aviation sector.[10] In particular, it observes that, even if the sector has long-established safety and security frameworks, these were created when focus on cybersecurity was less mature , as many traditional aviation technologies (e.g. radio-waves) used to be relatively exposed to less cybersecurity threats. Hence, operators are struggling to revise their practices and mindset.

The document outlines 4 steps to improve cybersecurity in the sector: the creation of global standards, more transparency, stronger collaboration, and information sharing practices. These are coherent with the results of other initiatives for the aviation sector. For instance, the Civil Aviation Organization (ICAO) released a draft "Aviation Cybersecurity Strategy," which lists seven pillars for a more secure aviation sector.[11] The ICAO General Assembly also adopted "Resolution A40-10: Addressing Cybersecurity in Civil Aviation," which reaffirms the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber threats and calls upon States to implement the ICAO Cybersecurity Strategy.[12]

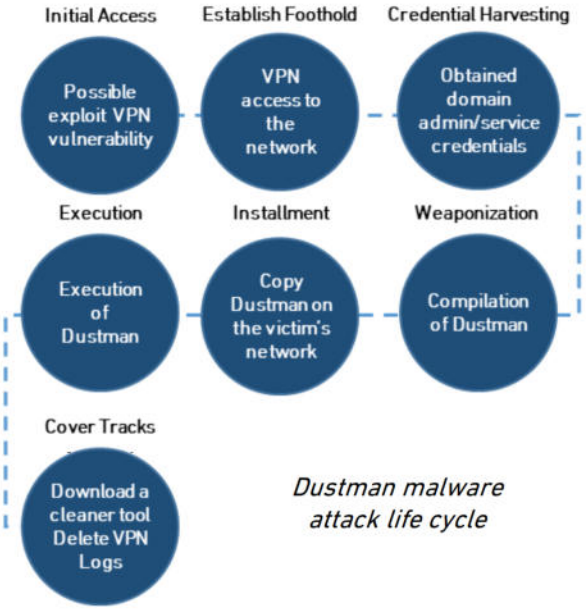
[7] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2019, October 2019.
[8] SonicWall Capture Labs, October 2019.
[9] Europol, Europol Publishes Law Enforcement and Industry Report on Spear Phishing, November 2019.
[10] Atlantic Council, Aviation cybersecurity: Scoping the challenge, December 2019.
[11] ICAO, Aviation Cybersecurity Strategy, October 2019.
[12] ICAO, Resolutions Adopted At The 40th Session Of The Assembly, October 2019.

National Cyber Outlook

Cybersecurity headlines regarding the Kingdom of Saudi Arabia

Saudi National Cybersecurity Authority discover a new wiper malware

At the end of 2019, the Saudi National Cybersecurity Authority (NCA) announced the discovery of a new malware named "Dustman." It is a type of "wiper" malware, which works by erasing the contents of affected storage devices. The malware is believed to have been used in a string of destructive attacks in late 2019, which targeted multiple entities across the Middle East.



Dustman malware attack life cycle

The investigation revealed that the malware appeared in July 2019, when it began to compromise the systems of its targets, while remaining sophisticated enough to bypass standard antivirus detection.

In addition to a thorough analysis of the malware's history and modus operandi, the NCA provided recommendations to help organizations mitigate the risks. These include 16 preventative (such as keeping an adequate level of cyber hygiene) and 12 detective measures (such as specification on what to keep monitored to timely detect the malware).[13]

G20: Security in the Digital Economy

The Kingdom of Saudi Arabia recently took over the G20 Presidency for 2020 from Japan at a meeting of the group's foreign ministers in Nagoya, Japan.

In alignment with the overall theme and goals of the presidency year, Security in The Digital Economy was identified as one of the priorities under the digital economy taskforce.

Saudi Foreign Minister, H.E. Prince Faisal bin Farhan Al Saud and his Japanese counterpart, Mr. Toshimitsu Motegi

Throughout 2020, the Digital Economy Task Force, will work on the outcomes of the Security in the Digital Economy priority along with B20, and related International organizations.

In the run-up to the Leaders' Summit, which will be held in November 2020, the Kingdom will host more than 100 meetings, including ministerial meetings and meetings of representatives from civil society.[14] A prominent example of this ambitious agenda is the much anticipated "G20 Cybersecurity Dialogue"[14]

[13] National Cybersecurity Authority, Destructive Attack "Dustman" Technical Report, December 2019.
[14] G20 official website.

Top Security Stories

A look at prominent cybersecurity event(s) from the last quarter

City of Pensacola[16]

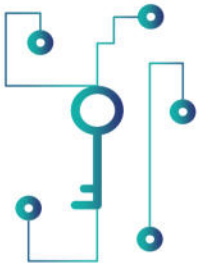
Location: United States

Sector: Public Administration

Date of disclosure: December 2019

Type of attack: Ransomware

Description: Pensacola, Florida, was hit by ransomware that affected its network (including phones and email at City Hall), and some online payment services (including Pensacola Energy).

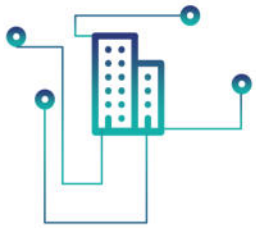


According to investigations, the ransomware was planted in Pensacola's system between the 5th December and 7th December, and was subsequently activated on the morning of December the 7th, affecting 27 systems.

The attacker leveraged two systems exposed to the internet. Once compromised, these two systems made it possible for the ransomware to propagate through the network.

Impact: The incident caused outages across a number of services, but essential ones (such as 911 and hospitals) were not impacted.

Attackers initially demanded a ransom of 3,750,000 SAR, then lowered it to 1,900,000 SAR. In December, attackers released 2GB of data stolen in the attack, stating they have more data from city networks.



The City's estimated cost related to the incident is 400,000 USD (approx. 1,504,000 SAR) as of January 31, 2020. Moreover, in order to build reserves for costs associated with the attack, the City of Pensacola decided to allocate extra 699,576 USD (approx. 2,632,000 SAR) to its internal insurance fund.

Lesson learned: This attack emphasizes the importance of building cyber resilience across all areas. The existence of appropriate backup measures and the incident management procedures will help to minimize the damages.

[16] City of Pensacola, Update on City of Pensacola Cyber Incident, Dec 2019; City of Pensacola, Comprehensive Annual Finanical Report, Financial Year 2019; City of Pensacola, Cyberattack FAQs , Dec 2019, City of Pensacola, Deloitte - Project Lurus, Jan 2020; Security Boulevard, Maze Ransomware Used in Pensacola Cyber Attack, Dec. 2019; CISO Magazine, Pensacola Ransomware: Hackers Release 2GB Data as a Proof Dec. 2019; Bleeping Computer, Ransomware Releases Files Stolen from City of Pensacola Dec. 2019.

Cyber Secure

In 2019, ransomware ranked as one of the most common attack techniques.17 For this issue, the NCA provides recommendations to minimize such risk

Prevent

- Back systems up regularly
- Keep devices patched and updated
- Use reputable antivirus, anti-phishing, and anti-spam software
- Manage software and user restriction policies
- Apply secure network design
- Use secure connections
- Use threat intelligence to anticipate ransomware campaigns

Detect

- Use Scan Email gateways
- Monitor for anomalous behavior, such as:
  - Poor spelling and grammar. The syntax may also seem unusual
  - Email addresses impersonating those of contacts
  - Unexpected requests to click on a link, download a file, or share personal information

Respond

- Start a ransomware removal process as soon as possible
- Disconnect devices from internet or local network
- Run a scan using security software
- Remove infected files from the network
- Restore data from the most recent backups

Recover

- Backup key data and applications to aid with a swift recovery
- Assess attacks and their root causes to identify lessons learned and improve prevention capabilities

The "Essential Cybersecurity Controls"

In 2018, the National Cybersecurity Authority of the Kingdom released its "Essential Cybersecurity Controls" (ECC). The goal of the ECC is to "set the minimum cybersecurity requirements for information and technology assets in organizations" in the Kingdom of Saudi Arabia.[18]

Organizations can refer to the ECC for controls and measures to minimize the cybersecurity risks that originate from internal and external threats.

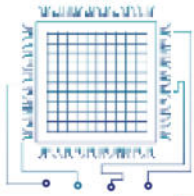
[17] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2019, October 2019.
[18] National Cybersecurity Authority, Essential Cybersecurity Controls (ECC – 1:2018).

Spotlight on Cyber Innovation

In this issue, the spotlight is on the cybersecurity implications of quantum computing

Despite dating back 30 years, the term "quantum computing" is now getting mainstream attention. Traditional computing devices, such laptops and smartphones, use binary digits, or bits, for their operations. These can only assume a value of either 0 or 1. In quantum computing, on the other hand, the basic unit is the qubit, which can assume a value of 0 and 1 at the same time. This allows quantum computers to operate at speeds exponentially faster than traditional ones, opening new possibilities for previously-impossible computing tasks.

In a recent experiment, a quantum computer performed a 3-minute calculation that, according to estimates, would have taken 10,000 years for a system with the computational power of 100,000 traditional desktop computers.[26] Such computational power could bring about huge changes for cybersecurity, particularly to the area of cryptography.



Potential Impact on modern cryptographic algorithms with quantum computing

26 algorithms potentially quantum resistant

Researchers are working to ensure cybersecurity for the quantum age. For instance, the US National Institute of Standards and Technology (NIST) shortlisted 26 algorithms to be tested, for "quantum resistant" algorithms.

Years are expected – according to optimistic estimates – in order to make quantum technology accessible at the consumer level.[28] However, organizations should get quantum-ready now. This is a long process, which could take decades for the most complex organizations – such as large organisations – to complete it.

Act now

Organizations should enhance data protection controls. In addition to encryption, data should be secured from unauthorized access, to ensure it's protected from "harvest and decrypt" techniques, which focus on gaining access to encrypted data, and storing it until it can be decrypted with quantum computers.[29]

Prepare for the future

Organizations should prepare for quantum computing with "crypto agility," which means the ability to continuously update cryptographic protection and algorithms in alignment with national cybersecurity standard. [31]

[26] Nature, Hello quantum world! Google publishes landmark quantum supremacy claim, October 2019.
[27] Craig Gidney *et al.*, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, December 2019.
[28] Spectrum, The Case Against Quantum Computing, November 2018.
[29] Deloitte, Technology, Media, Telecommunication Predictions, 2019.
[30] National Institute of Standards and Technology, Report on Post-Quantum Cryptography, April 2016.
[31] European Telecommunications Standards Institute, Quantum-Safe Cryptography (QSC).

This quarterly bulletin has been compiled by the National Cybersecurity Authority (NCA) of the Kingdom of Saudi Arabia (KSA). Its goals are to provide readers with an overview of the most important cybersecurity events and data from the quarter and to highlight the most interesting facts related to the focus of this issue. Aiming to :

- Elevate Cybersecurity knowledge and capabilities
- Provide outlook on latest cybersecurity trends, threats & risks

This report contains the information from several parties and individuals, noting that all information included in the report is indicative only. Also, the NCA does not bear any responsibility - under any circumstances - towards any party as a result of any decision or action taken or will be taken by that party based on the content of this report. The NCA asserts that it is not completely or partially responsible for any direct or indirect prejudice may occur.

About the NCA

The National Cybersecurity Authority (NCA) was established in 2017. The NCA is the government entity in charge of cybersecurity in Saudi Arabia and it serves as the national authority on all related affairs. It has both regulatory and operational functions related to cybersecurity and works closely with public and private entities to improve the cybersecurity posture of the country in order to safeguard its vital interests, national security, critical infrastructures, high-priority sectors, and government services and activities

https://nca.gov.sa @NCA_KSA